Federal Risk and Authorization Management Program (FedRAMP)

3PAO Program Overview

Matthew Goodrich
FedRAMP Program Manager
GSA Office of Citizen Services and Innovative Technologies

GSA®

FedRAMP℠

FedRAMP and the Security Assessment and Authorization Process

FedRAMP

- Maintains Security Baseline including Controls & Continuous Monitoring Requirements
- Maintains Assessment Criteria
- Maintains Active Inventory of Approved Systems

Consistency and Quality

1 Assessment

Independent Assessment

- Before granting a provisional authorizations, Cloud Service Provider systems must be assessed by an accredited 3PAO Third Party Assessment Organization

Trustworthy & Re-useable

2 Provisional Authorization

Grant Provisional Authorization

- Joint Authorization Board reviews assessment packages and grants provisional authorizations
- Agencies issue ATOs using a risk-based framework

Near Real-Time Assurance

3 Ongoing A&A (Continuous Monitoring)

Continuous Review of Risk

- Oversight of the Cloud Service Provider's ongoing assessment and authorization activities with a focus on automation and near real time data feeds.

Independent Assessments

1. CSPs must retain an independent assessor from FedRAMP accredited list of 3PAOs

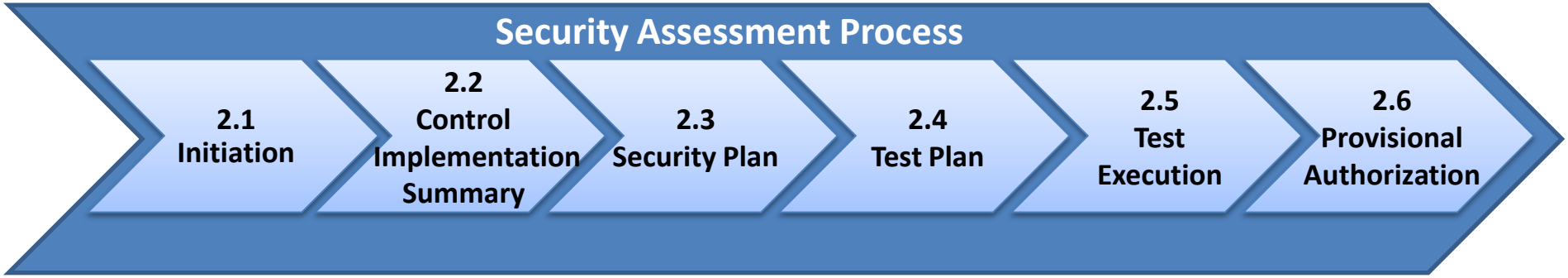
Authorizations:

1. Provisional ATO - Joint Authorization Board
2. ATO – Individual Agencies

Ongoing A&A Activities Will Be Coordinated Through:

1. DHS – CyberScope Data Feeds
2. DHS – US CERT Incident Response and Threat Notifications
3. FedRAMP PMO – POA&Ms

FedRAMP Security Assessment Process



- All templates, guidance, requirements will be publicly available
- Aligns with NIST SP 800-37 Risk Management Framework
- This is the same process flows CSPs would follow with individual agencies

FedRAMP Third Party Assessment Organization (3PAO) Conformity Assessment Process

FedRAMP requires CSPs to use Third Party Assessment Organizations (3PAOs) to independently validate and verify that they meet FedRAMP security requirements

FedRAMP worked with NIST to develop a conformity assessment process to accredit 3PAOs.

This conformity assessment process will accredit 3PAOs according to two requirements:

(1) Independence and quality management in accordance with ISO standards; and
(2) Technical competence through FISMA knowledge testing.

Benefits of leveraging a formal 3PAO approval process:

Creates consistency in performing security assessments among 3PAOs in accordance with FISMA and NIST standards

- Ensures 3PAO independence from Cloud Service Providers in accordance with international standards
- Establishes an approved list of 3PAOs for CSPs and Agencies to choose when satisfying FedRAMP requirements.